

DIRECTOR OF CENTRAL INTELLIGENCE

Security Committee

SECOM-A-251

13 January 1983

AGENDA

Two Hundred and Fifty-ninth Meeting
Wednesday, 26 January 1983, 10:00 a.m.
Room 4E64, Langley Headquarters Building

Preliminary Comments (e.g., status of terms of reference on leaks)

ITEM 1 Approval of minutes of 17 November, 3 December and 5 January meetings

ITEM 2 Subcommittee reports

ITEM 3 Presentation by Chairman, Personnel Security Subcommittee on
draft revision of DCID 1/14, and decision by members on it

ITEM 4 Report (member concurrence/comment on attached
draft revision of proposed SECOM response to FBI concerning
this report)

25X1

ITEM 5 New Business

ITEM 6 Next Meeting - tentatively scheduled for 10:00 a.m.,
23 February 1983

Attachment

Official Use Only When
Separated from Attachment

05 3 0137

CONFIDENTIAL

~~CONFIDENTIAL~~D R A E T

DIRECTOR OF CENTRAL INTELLIGENCE

Security Committee

SECOM-D-012

DATE

MEMORANDUM FOR: Mr. Edward J. O'Malley
Assistant Director, Intelligence Division
Federal Bureau of Investigation

FROM:
Chairman

25X1

SUBJECT: TAYLORMAID

25X1

1. Thank you for sharing with the Security Committee the report prepared by the TAYLORMAID working group. It is a welcome step in addressing the hostile technical penetration threat in the United States.

25X1

2. When they become available, the responses of the Army's 902nd Military Intelligence Group and the Air Force's Office of Special Investigations to your working group's tasking would be of interest.

25X1

3. The technical threat clearly is a matter requiring additional attention. The SECOM will be considering ways to assist in alleviating the problem posed by limited security resources, significant vulnerabilities, and a threat whose dimensions are not easily defined.

25X1

25X1

25X1

~~CONFIDENTIAL~~

SECRET

~~SECRET~~**ROUTING AND RECORD SHEET****SUBJECT:** (Optional)**FROM:**

Chairman, SECOM

EXTENSION**NO.**

25X1

DATE 25 January 1983

25X1

TO: (Officer designation, room number, and building)**DATE****OFFICER'S INITIALS****COMMENTS** (Number each comment to show from whom to whom. Draw a line across column after each comment.)

25X1

1.
CIA Member, SECOMCopy of my briefing material
for 26 January 1983 SECOM meeting.

2.

3.

4.

5.

6.

7.

8.

9.

10.

11.

12.

13.

14.

15.

PRELIMINARY COMMENTS

1. THE DDCI NONCONCURRED IN OUR PAPER ON LEAKS. MR. MCMAHON TOLD MR. CASEY THAT HE THOUGHT THE COMMUNITY WAS JUST FLAILING AROUND ON THE SUBJECT AND WOULD CONTINUE TO DO SO UNLESS THE WHITE HOUSE PROVIDES GUIDANCE. A COPY OF OUR MEMO WITH MR. MCMAHON'S COMMENTS ON IT IS AT YOUR PLACE. AT THIS POINT, IT APPEARS THAT WE WILL HAVE TO WAIT FOR ACTION ON THE WILLARD REPORT AND CONTINUE TO HANDLE LEAKS REFERRED TO US IN THE TRADITIONAL WAY. I BELIEVE THE ONLY WAY TO GET ACTION IS THROUGH THE PROPOSED LEGISLATION TO CRIMINALIZE GOVERNMENT EMPLOYEE LEAKS.

2. THE PROGRAM PRESENTATIONS AT THE 3 DECEMBER MEETING SEEMED TO BE WELL RECEIVED. I BELIEVE IT WOULD BE USEFUL TO SCHEDULE OTHERS FOR THOSE SECOM ELEMENTS WHICH ARE CONCERNED WITH TECHNICAL MATTERS. IF MEMBERS AGREE, WE WILL ARRANGE A SPECIAL MEETING IN A MONTH OR TWO TO HEAR PRESENTATIONS BY THE R & D SUBCOMMITTEE AND THE SECURITY ADVISORY GROUP USSR. R & D PROVIDES THE EQUIPMENT AND TECHNIQUES FOR USE IN MOSCOW, THUS MAKING CONSECUTIVE PRESENTATIONS LOGICAL. IT DOES NOT APPEAR THAT WE NEED PRESENTATIONS BY THE OTHER SUBCOMMITTEES AS THEIR WORK SEEMS ADEQUATELY BRIEFED TO MEMBERS THROUGH PRESENTATIONS AT REGULAR MEETINGS.

3. THE IG/CM HAS INDICATED THAT WILL CONDUCT FURTHER STUDY OF THE NEED FOR NEW NATIONAL POLICY ON TSCM.

25X1

4. THE IC STAFF IS STUDYING THE COMPUTER SECURITY PROBLEM AND THE D/ICS HAS INDICATED HE IS CONSIDERING APPOINTING A NEW

INTERAGENCY BODY WITH AN INDEPENDENT CHAIRMAN TO MAKE RECOMMENDATIONS. COPIES OF MY PAPER ON COMPUTER SECURITY TO ADMIRAL BURKHALTER ARE AT YOUR PLACES.

5. I AM PLEASED TO WELCOME BOB ALLEN AS THE FULL NAVY MEMBER. MY CONGRATULATIONS TO BOB ON HIS PROMOTION.

6. THE IC STAFF HAS BEEN REORGANIZED. THE ONLY WAY THIS AFFECTS SECOM IS THAT I NOW REPORT DIRECTLY TO THE DIRECTOR, IC STAFF, RATHER THAN THROUGH THE OFFICE OF COMMUNITY COORDINATION, WHICH HAS BEEN ABOLISHED. COPIES OF MY MEMO TO DC/ICS RE SECOM IMPLEMENTATION OF THE REORGANIZATION ARE AT YOUR PLACES.

7. YOU WILL FIND AT YOUR PLACES COPIES OF CORRESPONDENCE BETWEEN ME AND MR. KLEKNER, DIRECTOR OF SECURITY AND SAFETY, GENERAL ACCOUNTING OFFICE. GAO SEEMS TO BE MUCH MORE ACTIVE IN SECURITY MATTERS THAN THEY USED TO BE.

8. LAST MONTH I SENT MEMBERS A MEMORANDUM ASKING FOR NOMINATIONS TO FILL THE TWO STAFF POSITIONS PREVIOUSLY HELD BY AIR FORCE, ARMY, NAVY, DEFENSE, ENERGY, FBI AND JUSTICE HAVE RESPONDED NEGATIVELY. CIA HAS NOMINATED AN OFFICER EXPERIENCED IN COMPUTER AND TECHNICAL SECURITY. NSA ADVISES THAT THEY WILL NOMINATE TWO OFFICERS. WE HAVE NOT HEARD FROM STATE, TREASURY, DIA OR OSAF. WHEN I RECEIVE THE NSA NOMINATIONS, AND ANY OTHERS WHICH MAY BE SUBMITTED SOON, I WILL FORWARD THEM TO MEMBERS FOR INFORMATION AND COMMENT. BECAUSE THE SECOM PROFESSIONAL STAFF NOW CONSISTS OF DON PASCHAL AND ME, WE NEED TO FILL THESE SLOTS AS SOON AS POSSIBLE.

25X1

9. BASED ON EARLIER DISCUSSION WITH MEMBERS, I AGREED TO

SPEAK TO A MEETING OF THE INDUSTRIAL SECURITY WORKING GROUP. I DECLINED THEIR INVITATION TO DO SO AT THEIR MEETING IN CALIFORNIA BECAUSE OF OBJECTIONS BY A SECOM MEMBER. I HAVE AGREED TO SPEAK TO THEM AT THEIR 15 FEBRUARY MEETING AT AN APPROVED CONTRACTOR FACILITY IN THE D. C. AREA. MY PRESENTATION WILL BE LIMITED TO THE SECRET LEVEL, AND WILL FOCUS ON SECOM ORGANIZATION, FUNCTIONS AND SELECTED CURRENT ISSUES. I PLAN TO TELL THEM WE WOULD WELCOME INPUT FROM THEM ON SECURITY MEASURES WHICH AFFECT INDUSTRY, AND TO REMIND THEM ONCE AGAIN THAT THE ISWG DOES NOT ENJOY A POSITION AS A PART OF THE SECURITY COMMITTEE. THE RELATIONSHIP IS OF AN INFORMATIONAL NATURE EXCLUSIVELY.

10. WE MAY BE MOVING FROM THE HEADQUARTERS BUILDING LATER THIS YEAR, PROBABLY TO ROSLYN OR PERHAPS TO THE TYSON'S AREA. WE'LL KEEP YOU POSTED ON THIS.

11. A MOU HAS BEEN CONCLUDED WITH STATE DEPARTMENT REGARDING ITS ASSUMPTION OF PRIMARY RESPONSIBILITY FOR THE NEW MOSCOW EMBASSY SECURITY PROJECT.

12. THE NATIONAL COMMUNICATIONS SECURITY COMMITTEE HAS PROPOSED ESTABLISHMENT OF A WORKING GROUP OF THE CHAIRMEN OF SCOCE, SECOM'S TSCS AND AUDIO COUNTERMEASURES WORKING GROUP, AND POSSIBLY OTHERS TO DEVELOP A PLAN FOR MORE UNIFORM APPLICATION OF TECHNICAL SECURITY RESOURCES. THIS WAS IN RESPONSE TO TASKING FROM THE IG/CM FOR A REVIEW OF TEMPEST STANDARDS.

13. WE HAVE BEEN NOTIFIED BY THE PROTOCOL OFFICE THAT

WOULD LIKE ANY INTERESTED MEMBERS OF THE SECOM TO BE INVITED TO HIS AWARD CEREMONY ON FEBRUARY 1 IN HEADQUARTERS AUDITORIUM AT 11:00. IF YOU WOULD LIKE TO ATTEND OR SEND A REPRESENTATIVE FROM YOUR OFFICE, PLEASE LEAVE NAMES WITH

25X1

25X1

Page Denied

Next 1 Page(s) In Document Denied

CONFIDENTIAL

DIRECTOR OF CENTRAL INTELLIGENCE

Security Committee

SECOM-D-006

14 January 1983

MEMORANDUM FOR: Director of Central Intelligence

VIA: Deputy Director of Central Intelligence
Director, Intelligence Community Staff

FROM:

Chairman

SUBJECT: Initiatives to Deal with Leaks

1. Action Requested: Your review and approval of the attached terms of reference on Community initiatives to deal with the problem of unauthorized disclosures of classified intelligence information.

2. Background: On 22 December 1982, you asked for an early meeting of the Security Committee to address initiatives to combat leaks that would be supported by the Community and to prepare terms of reference to implement them.

3. Current Status: SECOM met on 5 January 1983 in response to your tasking. Initiatives supported by all Community agencies represented on the SECOM are summarized at Tab A. Draft terms of reference to implement the agreed initiatives are at Tab B.

4. Recommendation: That the DCI approve the attached draft terms of reference for initiatives to deal with leaks of intelligence.

Attachments

Regraded Official Use Only When
Separated from Attachment

CONFIDENTIAL



CONFIDENTIAL

SUBJECT: Initiatives to Deal with Leaks

CONCUR:

Director, Intelligence Community Staff

*now - CONCUR - WE'RE
PREPARING TO TALK GUYS
IN CHURCH*

Deputy Director of Central Intelligence

18 JAN 1983

Date

20 JAN 1983

Date

APPROVAL:

Director of Central Intelligence

Date

25X1

CONFIDENTIAL

CONFIDENTIAL

SUBJECT: Initiatives to Deal with Leaks

Distribution:

Orig - Return C/SECOM w/att

1 - DCI w/att

1 - DDCI w/att

1 - ExDir w/att

1 - ER w/att

1 - D/ICS w/att

1 - ICS Registry w/att

1 - C/UDIS w/att

CONFIDENTIAL

Page Denied

Next 2 Page(s) In Document Denied

OFFICIAL USE ONLY
DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

SECOM-D-019

24 January 1983

MEMORANDUM FOR: Chairman, DCI Information Handling Committee
Chairman, SECOM Computer Security Subcommittee

FROM:

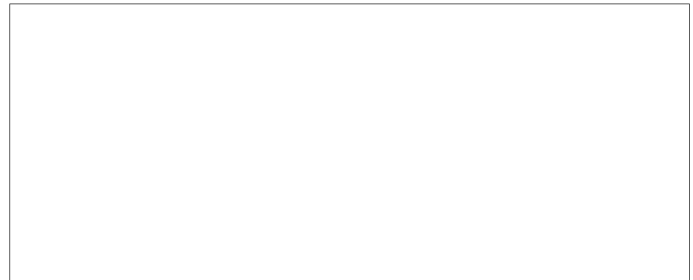

Chairman

STAT

SUBJECT: Computer Security

Attached for your information is a copy of a paper I sent the Director of the Intelligence Community Staff concerning policy structures to support computer security.

Attachment



STAT

CONFIDENTIAL

DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

SECOM-D-017

21 January 1982

MEMORANDUM FOR: Director, Intelligence Community Staff

FROM:

Chairman

25X1

SUBJECT: Computer Security

1. This paper responds to the request for proposals to create a policy structure to support computer security in the coming period of exponential growth in the applications of computer technology, the numbers of people who will have access to the computerized data and/or the hardware and software, and the components which will access Community-wide networks handling sensitive intelligence and information on sources and methods.

2. The measures contemplated include terms of reference for Community guidance in computer security matters; determination of appropriate Community roles for the DoD Computer Security Evaluation Center, the National Communications Security Committee, the DCI Information Handling Committee, the DCI Security Committee's Computer Security Subcommittee, the Intelligence Community Staff, and of the NFIB and NFIC agencies; establishment of long- and short-range goals for computer security; Community policy for computer security; consideration of means of obtaining the support of the computer industry for development of more-easily-secured systems; establishing requirements for U. S. collection of intelligence concerning hostile efforts and capabilities to penetrate our computer systems and ensuring optimum utilization of all such intelligence collected; formulating uniform training for computer security specialists; and a forum and mechanism for the consideration and solution of computer security issues and problems.

3. Computer security resources, both human and financial, are in short supply and likely to remain so for the immediate future. Those with expertise in computer security are heavily burdened with their own agencies' efforts and have little time to spare for Community work. The SECOM Computer Security Subcommittee is a prime example of this problem. Now that computer security has been "discovered" by the Community, however, it is possible that managers will be willing to contribute more of their people's time, effort and expertise. Nevertheless, Community agencies would be hard pressed to contribute security experts to serve on a full-time task for an extended period of time.

OFFICIAL USE ONLY When
Separated From Attachment

CONFIDENTIAL

CONFIDENTIAL

4. It is essential that any group charged with laying the groundwork for computer security for the Intelligence Community through the nineteen-eighties embody the broadest possible representation. The military services' desire to make as much data as possible available to tactical commanders must be considered along with the Clandestine Services' desire to assure maximum protection of sources and methods. It is also important that the structure for computer security policy have close ties with similar groups concerned with the other essential security disciplines: personnel, physical, technical, and procedural, as well as COMSEC and emanations security. Finally, the group should have a Community-recognized role and charter to act on behalf of the DCI in formulating policy proposals for his consideration.

5. This paper, therefore, is a proposal to use an existing institution to deal with a problem properly under its jurisdiction. The charter (attached) of the Computer Security Subcommittee under DCID 1/11 assigns to it the major part of the responsibilities discussed above. With computer security's elevation to greater prominence, it should now be possible to obtain the cooperation needed to deal with it effectively. As stated earlier, it is unlikely that the members of the subcommittee can be spared full-time by their organizations, but they should be able to devote appreciably more time and effort to the subcommittee.

6. The DoD Computer Security Evaluation Center is represented on the Computer Security Subcommittee. At least one member is also a member of the NCSC. I would suggest that observers from the Information Handling Committee, the Technical Surveillance Countermeasures Subcommittee and the NCSC be added to the subcommittee to ensure input from these sectors. To enhance information sharing, I propose that a SECOM Staff member be afforded observer status on the IHC, NCSC and the TTIC/Department of Commerce Working Group, during any deliberations of these bodies on computer security matters.

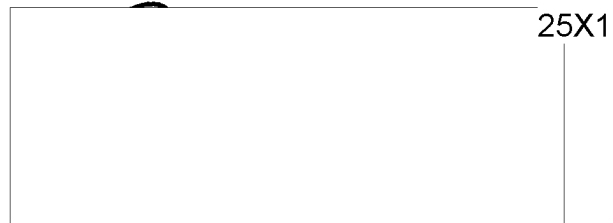
7. Recognizing that some full-time staff assistance is needed, I have taken steps to recruit a computer security specialist to fill one of the vacant slots on the SECOM Staff. Because of other duties of the position, I do not believe that one person will be able to provide all of the needed support. I do believe, however, that the addition of one more computer-security-knowledgeable individual to the SECOM Staff would provide sufficient support to the Computer Security Subcommittee to make headway against the tasks that now cry out for action. This was the minimum level recommended in the paper produced by the Policy and Planning Staff.

8. I agree that throwing resources at the problem is not the solution, especially since significant resources are not available in the near term. But I am convinced that, with the exercise of leadership from the D/ICS level or above and the investment of limited resources, progress is possible in most areas of computer security through the efforts of the Computer Security Subcommittee and the SECOM Staff.

CONFIDENTIAL

CONFIDENTIAL

9. Your favorable consideration of the above proposal is requested.



Attachments

DCID No. 1/11 Attachment 2

DCID No. 1/16

CONFIDENTIAL

SECRET

DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

SECOM-D-018

24 January 1983

MEMORANDUM FOR: Deputy Director, Intelligence Community Staff

FROM:

[redacted]
Chairman

25X1

SUBJECT: Staff Planning (U)

REFERENCE: Your 13 January 1983 Note, Same Subject

As we discussed [redacted] the Intelligence Community Staff reorganization, except for the dissolution of the Office of Community Coordination, will have minimal structural impact upon the Security Committee. We have operated in the past in general accordance with the reorganization. [redacted]

25X1

25X1

The SECOM will continue to provide a mechanism for Community-wide planning, management and coordination of a broad array of security issues. We will ensure every member an opportunity to be heard on every topic before the Committee, and the Staff will provide independent positions that best serve the interests of the DCI and the Community. We will seek the best qualified people for staff assignments and subcommittee appointments. [redacted]

25X1

As security problems become increasingly involved with high technology systems, security costs can be expected to increase, making practicable solutions even more difficult within the constraints of limited resources. The involvement of the SECOM membership in the issues addressed may be expected to continue at a high level, as these issues are varied and comprehensive, affecting all segments of the Community at all levels. [redacted]

25X1

The initiatives raised in the SECOM are viewed by the members on the basis of their particular priorities and equities. Generally, they all perceive the same problems. Solutions are often a different matter. Yet consensus is possible and often effective. The SECOM consensus on personnel security investigations was instrumental, I believe, in substantially altering a trend in the DoD toward less stringent investigations. It was effective in obtaining DDCI action to dissuade the Department of Energy from contracting out the staff of its all-source intelligence communications center. [redacted]

25X1

SECOM is structured to address most of the major security issues of concern to the Community through eight subordinate elements, each representing all interested Community components. They are:

CL BY SIGNER
DECL OADR

SECRET

SECRET

1. Compartmentation Subcommittee - Chaired by Air Force. Reviews, develops and coordinates security policy and procedures on the handling and use of sensitive compartmented information and data relating to intelligence sources and methods. This subcommittee will review and revise, as needed, Community security procedures on handling and use of sensitive compartmented information (SCI) and source and method data, and update hazardous area lists applicable to foreign travel by persons with sensitive access. []

25X1

2. Computer Security Subcommittee - Chaired by DIA. Reviews, develops and coordinates Community security policy for the protection of intelligence processed by or stored in ADP systems. During 1983 this subcommittee will complete a revision of the DCI computer security policy paper; will review, refine and revise, as needed, Community collection requirements on hostile threats to computers; and will conduct other related activities as determined by the ongoing IC Staff review of computer security. []

25X1

3. Personnel Security Subcommittee - Chaired by NSA. Reviews, develops and coordinates Community security policy and procedures for the investigation and adjudication of the eligibility of persons proposed for access to sensitive intelligence. This subcommittee will complete an ongoing revision of DCI personnel security policy for access to SCI; conduct three seminars for Community personnel security officers who adjudicate investigative data for SCI access determinations; and participate in studies and analyses of polygraph techniques. []

25X1

4. Research and Development Subcommittee - Chaired by CIA/ORD. Plans, coordinates and monitors research and development on matters of security concern to the Community. During 1983 the R&D Subcommittee will continue R&D projects to support State Department management of the Moscow security program; arrange for R&D on an advanced countermeasures receiver for Community use in technical surveillance countermeasures inspections; and sponsor R&D on a variety of security matters (e.g., RF emanation detection and location). []

25X1

5. Security Advisory Group USSR - Chaired by State. Plans and coordinates Community support for the State Department program to safeguard the new U. S. Embassy being constructed in Moscow. During 1983 the SAG-USSR will arrange support for the security inspection of Soviet-made and installed building components and for security measures to protect sensitive US components being installed in the new building. []

25X1

SECRET

SECRET

6. Security Awareness Subcommittee - Chaired by FBI. Develops and coordinates security awareness and education materials for use by the Community in briefing on the hostile threat and on measures to avoid compromise. During 1983 the subcommittee will arrange for the development of security awareness briefings and materials; catalog for the benefit of the Community security awareness materials developed by departments and agencies, contractors, and allied countries; and study means of influencing opinion, within government and outside, against unauthorized disclosures of classified intelligence and those who perpetrate such leaks. [REDACTED]

25X1

7. Technical Surveillance Countermeasures Subcommittee - Chaired by CIA/OS/TSD. Coordinates U. S. Government defenses against hostile technical surveillance and conducts training for all Community personnel who conduct technical countermeasures inspections. During 1983 TSCS will update procedural guides for the Community on how to inspect for technical penetration and what to do with "finds"; oversee implementation of budgeted improvements to the Community's sole technical surveillance countermeasures training facility; sponsor security testing of new computerized telephone systems; and improve screening procedures for the review of license requests for the export of countermeasures equipment. [REDACTED]

25X1

8. Unauthorized Disclosures Investigations Subcommittee - Chaired by CIA/OGC. Provides a focal point for the Community to coordinate investigations of unauthorized disclosures of intelligence, and seeks to develop security procedures to preclude the recurrence of leaks. During 1983 UDIS will evaluate document control technology and methods for preventing leaks of extremely sensitive data; develop means to improve the quality, timeliness and Community coordination of leak investigations; and seek to develop a plan of action for sharing damage assessments among agencies. [REDACTED]

25X1

I believe that completion of the planned tasks identified above will significantly enhance the security of the Community in ways that are practicable and acceptable to Community components. Unless otherwise directed, I will proceed according to this plan during 1983, and will use existing structures to address new initiatives from SECOM members and any specific tasking received during the year. [REDACTED]

25X1

25X1

DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

SECOM-D-414

29 December 1982

Mr. Arthur A. Klekner
Director, Office of Security and Safety
General Accounting Office, Room 4844
441 G Street, N. W.
Washington, D. C. 20548

Dear Mr. Klekner:

Thank you for your interest in the Security Committee's Adjudicators' Seminars. As [redacted] must have told you, the seminars are conducted for Intelligence Community adjudicators who evaluate cases involving access to sensitive compartmented information (SCI). A primary objective is to achieve a higher degree of homogeneity and constancy in SCI adjudications among the several agencies of the community.

STAT

The seminars have been consistently oversubscribed, and we are anxious to afford those for whom the course was designed the earliest opportunity to attend, thereby achieving our primary objective. It is my understanding that the SCI adjudications for the General Accounting Office are performed within the Intelligence Community.

I would suggest we arrange for one GAO security officer to attend the seminar in March to evaluate its potential worth to your organization. It may turn out that such a specialized program is not what you are seeking. If it appears to be worthwhile, we will try to arrange attendance by other GAO personnel as permitted by Intelligence Community requirements. If you will provide the name of a candidate, I will arrange for enrollment. If you wish to discuss this proposal, please call me on [redacted]

STAT



UNITED STATES GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

OFFICE OF SECURITY

December 22, 1982

[redacted]
Chairman, DCI Security Committee
Room 5E25
CIA Headquarters
Washington, DC 20505

STAT

Dear [redacted]

STAT

In November 1980, the U.S. General Accounting Office established an internal Office of Security & Safety. Although the mission of GAO does not place it directly in the intelligence community, we are making every effort to have our internal security procedures and standards no less than that of those agencies in the Executive Branch of the Government.

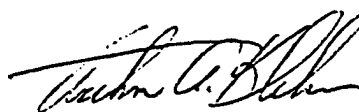
In 1979, the FBI, at the request of the Comptroller General, did a review of the overall security program in GAO. In March of this year, the new Comptroller General requested that the FBI re-review the security of GAO to determine if the previous recommendations had been established and/or followed and to make any further recommendations, as appropriate. One of the new recommendations the FBI will be making to the Comptroller General, is that the members of the Personnel Security Branch of the Office of Security & Safety attend the intelligence community adjudication conference.

I spoke with [redacted] of your staff, and he informed me there are a total of four conferences in 1983. This is to request two slots for the first conference, one for myself and one for the main adjudicator of my staff. Additionally, I would like to request two slots at any of the other three conferences.

STAT

If you have any questions, please feel free to contact me or Linda Skelly of my staff on 275-4700. I would appreciate your prompt attention to this matter.

Sincerely yours,


Arthur A. Klekner
Director

DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

SECOM-D-404

15 December 1982

Mr. Arthur Klekner
Director, Office of Security and Safety
General Accounting Office, Room 4844
441 G Street, N. W.
Washington, D. C. 20548

Dear Mr. Klekner:

Mr. Brown's letter of 30 November 1982, requesting assistance of the DCI in training GAO personnel in technical countermeasures, has been referred to me. The [redacted] operates under the sponsorship of the DCI Security Committee (SECOM). STAT

At this time, plans are underway to provide technical surveillance countermeasures training to the US Capitol Police, under sponsorship of the FBI. In order to maintain FBI cognizance of Legislative Branch TSCM training, I have forwarded Mr. Brown's letter to Mr. Lloyd E. Dean, Systems Program Manager of the FBI. I have asked Mr. Dean to contact you regarding GAO's request.

I regret the delay in responding, but Mr. Brown's letter did not reach me until 9 December. If I can be of assistance to GAO, please do not hesitate to contact me.

STAT

GAO

United States General Accounting Office
Washington, DC 20548

General Services and Controller

NOV 30 1982

Director, Central Intelligence Agency
Central Intelligence Agency
Washington, D.C. 20505
ATTN: SECOM

Dear Sir:

The General Accounting Office is comprised of a Headquarters, fourteen Regional Offices in the U.S. and three overseas offices. The mission of GAO frequently necessitate acquisition, storage, discussion and dissemination of classified/sensitive information obtained from both government and private organizations.

The wide access to classified/sensitive information which GAO auditors/evaluators are often afforded renders this organization extremely sensitive to potential targeting by hostile elements.

In 1980, the General Accounting Office established an Office of Security and Safety whose primary mission is to safeguard information and personnel within the agency. One project currently being implemented is the establishment of an effective countermeasure program. The Office of Security has procured several devices designed for use in this program to detect and locate RF transmission devices ("bugs"), and telephone analysis equipment. Instruction in the use of this equipment was provided by the vendors from whom the equipment was purchased.

In order to create and implement a highly effective countermeasure program for the GAO, highly specialized and intensive training is necessary. The nature of the training we are interested in is not limited to proper use of countermeasures equipment, but also in the development of a total program. Such a program would include, but not be limited to, recognition of the threat, proper physical search technique, identification of clandestine listening devices and telephone taps, establishment of preventive measures against such possible attacks and any other information and training that would serve us in establishing a credible countermeasures program.

While we, as an agency, do have some limited expertise in-house to establish such a program, we do not feel that our current level of knowledge is adequate to the task. However, it has come to our attention that training in this field is available only through the intelligence community through agencies such as yours.

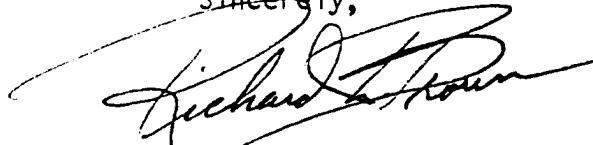
In view of the above, it is requested that this office be authorized to send representatives to your training center to obtain the necessary



instructions regarding establishment of a total countermeasures program for the GAO. We have previously discussed this matter with personnel at your training site and have been advised to request this training through your Headquarters. Any assistance you can give us in this matter would be greatly appreciated.

Please direct your response to this inquiry to the Director, Office of Security and Safety, General Accounting Office, 441 G Street, N.W., Room 4844, Washington, D.C. 20548, phone (202) 275-4700.

Sincerely,

A handwritten signature in dark ink, appearing to read "Richard L. Brown", with a large, sweeping flourish extending from the end of the signature.

Richard L. Brown
Director

Page Denied

Next 2 Page(s) In Document Denied



POLICY

THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

In reply refer to:

I-14473/82

22 SEP 1982

MEMORANDUM FOR GENERAL STILWELL

SUBJECT: Survey of Special Background Investigation (SBI)
15 Year Period of Coverage-INFORMATION MEMORANDUM

On 15 June 1982, the Army, Navy, Air Force and DIS were tasked to conduct a two month survey (1 Jul 82-31 Aug 82) to determine how far back the SBI must go in order to uncover adverse information serious enough to warrant denial of access. This survey was prompted by two factors: (1) the Select Panel recommendation for DoD adoption of a single scope background investigation at the level mandated by DCID 1/14 and (2) the impact that such an investigative effort would have on DIS considering the required 15 year period of coverage for an SBI.

It has long been our position that a ten year investigative scope would be more than adequate coverage to reveal significant factors in a person's background that might affect their eligibility for access to sensitive compartmented information (SCI). In fact, the survey revealed that of the 7,385 total cases reviewed during the period, 213 were considered for an adverse action; of these only 2 cases were based on information developed exclusively in the over 10 year period. It also appears that in those instances the adverse information was of such a nature that it would have been uncovered in the course of a 10 year scope investigation or less.

As a result of this and other previous studies, and due to our concern over the impact that a single 15 year scope background investigation would have on DIS, a recommendation was made to the Personnel Security Subcommittee (PerSSub) of the DCI Security Committee (SECOM) to change DCID 1/14 coverage from 15 to 10 years. On 14 September 1982, the OSD proposal on this point was defeated by a vote of 7 to 5. However, I intend to pursue this action further directly with the SECOM principals and will keep you informed of my progress.

W. J. Maynard
Maynard C. Anderson
Director

Security Plans and Programs

Attachment

Bl 9/22

Summary of DoD Survey of SBI Period of Coverage

1. Adverse information appearing in only one year group category:

(1)	0 - 5 years:	166
(2)	6 - 10 years:	12
(3)	11 - 15 years:	1
(4)	16+ - years:	<u>1</u>

Total: 180

2. Adverse information appearing in more than one year group category:

(1)	0 - 5 years:	31
(2)	6 - 10 years:	29
(3)	11 - 15 years:	6
(4)	16+ - years:	<u>3</u>

Total: 69

3. Total of both the above categories:

(1)	0 - 5 years:	197
(2)	6 - 10 years:	41
(3)	11 - 15 years:	7
(4)	16+ - years:	<u>4</u>

Total: 249*

* This number totals more than 213 due to the fact that a number of cases reported adverse information in as many as three or four categories.

Page Denied

D R A F T

DIRECTOR OF CENTRAL INTELLIGENCE

Security Committee

SECOM-D-012

DATE

MEMORANDUM FOR: Mr. Edward J. O'Malley
Assistant Director, Intelligence Division
Federal Bureau of Investigation

FROM:

Chairman

25X1

SUBJECT:

TAYLORMAID (U)

1. Thank you for sharing with the Security Committee the report prepared by the TAYLORMAID working group. It is a welcome step in addressing the hostile technical penetration threat in the United States.

25X1

2. When they become available, the responses of the Army's 902nd Military Intelligence Group and the Air Force's Office of Special Investigations to your working group's tasking would be of interest.

25X1

3. The technical threat clearly is a matter requiring additional attention. The SECOM will be considering ways to assist in alleviating the problem posed by limited security resources, significant vulnerabilities, and a threat whose dimensions are not easily defined.

25X1

25X1

CL BY SIGNER
DECL OADR

CONFIDENTIAL

Page Denied

Next 2 Page(s) In Document Denied

CONFIDENTIAL

14 JAN 1983

MEMORANDUM FOR: Chairman, DCI Security Committee

FROM:

[redacted]
CIA Member
DCI Security Committee

25X1

SUBJECT:

[redacted]
Rotational Assignment Nomination [redacted]

25X1

25X1

1. I am pleased to nominate [redacted] Security Officer, for the position of Deputy for Technical Security, SECOM. [redacted] is an experienced senior security officer with broad knowledge of physical, technical and information security matters. He is a self-starter. He communicates effectively both orally and in writing. His many years in computer security make him, by Agency standards, an exceptional candidate for this position. [redacted]

25X1

25X1

25X1

2. A brief biographic sketch of [redacted] is attached. He is very enthusiastic regarding his candidacy. It would be appreciated if you would advise this Office [redacted] is the successful candidate for this position so that the necessary arrangements for his rotational assignment can be made. [redacted]

25X1

25X1

25X1

25X1

Attachment

WARNING NOTICE
INTELLIGENCE SOURCES
OR METHODS INVOLVED

CONFIDENTIAL

25X1

Page Denied



United States Department of State

Assistant Secretary of State
for Administration

Washington, D. C. 20520

OD/A Registry
83-0336

SECRET

January 21, 1983

Dear Harry:

I regret the delay in responding to your letter of January 17, but I have been travelling and have just returned to the office.

I appreciate your drafting the proposed Memorandum of Understanding. I concur in your approach, and have signed the original. Enclosed is a copy for your records.

The Department looks forward to continued cooperation and support from the Agency and the DCI Security Committee in order to insure the continuity and successful completion of this important project.

Sincerely,

Thomas M. Tracy

Enclosure:

As stated.

The Honorable
Harry E. Fitzwater,
Deputy Director for Administration,
Central Intelligence Agency.

SECRET
DECL: OADR

Page Denied

Next 2 Page(s) In Document Denied